International Journal of Innovative Research in Science and Technology
Volume 01, Issue 01, August 2021
www.ijirst.com

Review on Cloud Computing Security Solutions against Various Issues

T. Ashok[1], K. Suresh[2]
[1,2](Department of CSE, Geetanjali Institute of Technology, Vijayanagaram, Andhra Pradesh, INDIA)
Corresponding Author: ashokt019@gmail.com

To Cite this Article
T. Ashok and K. Suresh, "Review on Cloud Computing Security Solutions against Various Issues", International Journal of Innovative Research in Science and Technology, Vol. 01, Issue 01, August 2021, pp.:015-021.

Abstract: *Cloud storage, a rapidly developing digital technology, has piqued the attention of the whole world. Cloud computing is Internet-based computing in which common services, applications, and information are provided to machines and devices on demand, such as the power grid. Cloud computing is the outcome of the confluence of traditional computer technologies with network technology, such as grid computing, distributed parallel computing, and so on. Cloud storage has piqued people's attention. Cloud infrastructure is being sought by an increasing number of companies and government agencies. With the growing use of cloud storage, however, security issues have emerged on a larger scale. It's critical to solve these security issues in order to persuade more people to utilize cloud computing. The goal of this study is to identify the most vulnerable security risks in cloud computing, so that both end-users and providers may learn about the main security dangers that come with it. This will motivate researchers and security professionals to learn more about the requirements of customers and suppliers, as well as critically evaluate the many security models and technologies that have been suggested.*

Keywords*: Grid computing, middleware, replication, hazards, virtualization, cryptography*

I. Introduction

The Internet has become a driving force in the development of a wide range of technologies. Among all of them, cloud infrastructure is probably the most contentious. Cloud infrastructure is seen as a development in the contemporary situation by almost all businesses wanting to enter it. The cloud is developing as a new approach to handle alternative distribution methods with IT skills. It's a way of delivering IT-enabled services in the form of applications, networks, and more.

"A computing cloud is a set of network-enabled resources that comprise scalable, Quos-assured, usually configurable, cheap on-demand computing platforms that can be accessed in an easy and ubiquitous way," according to Wikipedia[1]. In simple words, cloud infrastructure is the synthesis of a technology and a network that provides Internet hosting and storage services. Inquire about device infrastructures that provide enough service. Cloud Infrastructure is the introduction of technical ideas in order to access high-quality software via the Internet. Cloud computing's main goal is to provide high-quality service levels with flexible and cost-effective on-demand computing infrastructures. Cloud computing supports internet-based, highly flexible distributed computer systems in which intellectual services are provided as a commodity. Allowing the usage of cloud infrastructure has the following advantages: (i) decreased hardware and maintenance costs, (ii) Global connectivity, as well as Flexibility and a completely automated procedure that eliminates the user's need to worry about app updates, which seems to be a common occurrence. It's critical to distinguish between the consumer and the cloud in cloud computing. In most cases, the customer connects to the cloud through the internet. It's also feasible to set up a private cloud inside an organization when a user is connected to an intranet. The client makes requests to the server, and the computer fulfills them. Multi-tenancy and elasticity are two key features of the cloud paradigm. Multi-tenancy enables several tenants to swap the same example of operation. Elasticity refers to the ability to change the amount of capital allocated to a service based on the current service requirements. Both characteristics are focused on maximizing energy efficiency, cost, and facility affordability.

II. Cloud Computing Architecture

When learning about a cloud storage system, it's helpful to divide it into two parts: the front end and the back end. They communicate with one another via a network, most often the Internet. The front end is the hand that the machine's owner, or customer, uses. The "cloud" of the system includes the back end.

Figure no 1: The architecture of cloud data storage service

The customer's computer and the software used to access the cloud storage infrastructure are both part of the front end. The user experience is not the same across all cloud storage apps. For utilities like Web-based e-mail programs, current online browsers such as Internet Explorer or Firefox are used. Other networks provide unique programming and network connection to their users. On the device's back end are the many computers, servers, and data storage facilities that make up the "cloud" of computing resources. A central server monitors traffic and client requests to ensure the gadget is functioning correctly. It adheres to a set of protocols and makes use of middleware, which is a kind of software. Middleware enables networked devices to communicate with one another. Most of the time, servers aren't running at full speed. A cloud storage system would create a backup of all of its users' knowledge and store it on other computers. Copies allow the central server to access backup machines and restore data that might otherwise be inaccessible. Replication is the process of making copies of data to use as a reference. Software as a service, network as a service, and service infrastructure are the three types of services that cloud platform providers seek to provide.

SaaS (Software as a Service):

To provide on-demand technological services. To access a single instance of the program, cloud apps with different end customers or client entities are utilized. Although Salesforce.com is the most well-known example of Seas, many other instances have emerged, including Google Applications' supply of basic corporate tools like as email and word processing. Though salesforce.com was a few years behind the cloud computing idea, it currently operates via its counterpart force.com, which may be described as a service gateway.

Peas (Application as a Service):

A framework as a service wraps a software layer and makes it available as a service that can be utilized to build higher-level applications. There are at least two perspectives on Peas, depending on the manufacturer's or user's point of view:

Anyone who makes Peas may build a network by integrating an operating system, middleware, application software, and even a production environment that is then sold to a customer as a service.

Those that utilize Peas will use an encapsulated service that is provided to them through an API. The user interacts with the application through the API, and the platform handles and scales it while maintaining a given level of service. Peas instances may be identified as virtual appliances. Commercial Peas examples may be found on the Google Apps Engine, which supports Google infrastructure programs. Pea's systems like these may provide a strong foundation for delivering applications, but the capabilities that the cloud provider chooses to offer may limit them.

Infrastructure-as-a-Service (Iasi):

As organized networks, infrastructure as a service provides critical storage and computing resources throughout the network. Computers, disc devices, switches, routers, and other systems are integrated and made useable in order to handle workloads ranging from device modules to high-performance computer devices. Joint, whose main product is a series of virtualized servers that provide an infrastructure that is highly usable on demand, is one commercial example of Iasi.

Risks in cloud infrastructure:

In the past several years, cloud storage has evolved from a potential business model to one of the IT industry's fastest growing industries. Businesses that have been struck hard by the recession are quickly discovering that they can have fast access to best-of-breed business applications and significantly increase their infrastructure

capacity by using the cloud, both at a low cost. However, as more and more personal and business data is stored on the cloud, concerns about its reliability are beginning to arise.

The Network's Security:

Problems and settings with network communications that are important to cloud storage systems. The ideal strategy for network security is to treat cloud providers as extensions of customers' existing internal networks [2], with the same safety procedures and security safeguards in place. And to make it possible to apply local methods to any remote resource or activity.

Transfer security:

More cloud data in transit is a result of distributed systems, massive resource sharing, and replication of virtual machine (VM) instances, necessitating VPN methods to protect the device from sniffing, spoofing, and man-in-the-middle and side-channel attacks.

Firewalling:

Firewalls protect the vendor's internal cloud resources from insiders and outside users [3]. They may frequently be used to identify VM separation, fine-grained filtering for addresses and ports, DoS protection, and external security assessment processes. Adaptation efforts.

A consistent firewall and associated security measures specific to cloud settings may be seen in the need to adapt existing technologies to this new software architecture.

Protective measures:

Configuring protocols, frameworks, and technologies to meet the required security and privacy requirements while preserving performance and efficiency [4].

III. Security Concerns

The cloud storage software provider must ensure that sensitive information about the customer is properly protected from all suppliers, clients, and consumers. Because most servers are external, the cloud service provider may control who has access to the data and who maintains the system, allowing the provider to protect the user's sensitive information.

Data protection:

Cloud data is stored in a variety of physical repositories around the globe, and data security is difficult to maintain in the absence of appropriate technical and legal constraints. To begin with, different regions, some ahead of others, have varying degrees of technology. Data is safe in one location, but it may be in jeopardy in another. Second, there are many laws in various sectors.

Interactions:

With cloud use and control, focus on user, technical, and programming interface issues.

API: Programming interfaces (important to Iasi and Peas) for accessing virtualized services and systems must be secured to prevent malicious use [5].

User interface for administrators:

Iasi (VM management) services, Peas (coding, deployment, and testing) development, and Seas framework tools may all be controlled remotely (user access control, configurations).

User-interface design:

For the investigation of the provided materials and equipment (the service itself), the end-user man recommends that environmental conservation measures be taken.

Authentication and verification:

Mechanisms that are required in order to get access to the cloud. As a consequence, most providers rely on standard accounts, which are susceptible to a variety of attacks, which are exacerbated by multi-tenancy and resource sharing.

Virtualization:

VM isolation, hypervisor problems, and other concerns with virtualization technology [6].

Isolation:

While nominally isolated, all VMs use the same hardware and, as a result, the same infrastructure, making it easier for hostile organizations to exploit data breaches and cross-VM attacks [7]. It's also essential to apply the separation concept to finer-grained characteristics like computational capital, storage, and memory.

Hypervisor vulnerabilities:

The hypervisor is the most important software component of virtualization. While hypervisors are recognized to have security flaws, solutions are still uncommon and largely proprietary, necessitating further research to strengthen these security components.

Information leakage:

Circumvent hypervisor vulnerabilities and lack of isolation measures to leak data from virtualized infrastructures, acquire sensitive customer data, and damage security and honesty.

Government:

Issues with cloud storage solutions (loss), as well as administrative and security measures. (8), (9) Uh,

I keeping track of specifics:

When you move data to the cloud, you lose the power of redundancy, location, file systems, and other critical variables.

Security Management:

Although inadequate Service Level Agreements (SLA) lead to security vulnerabilities, the loss of protective frameworks and policies governed as terms of use hinder customer-side vulnerability assessment and penetration testing.

Data transfer security:

All traffic from your network and any services you use in the cloud would be routed via the Internet. Make sure your data is still sent over a secure channel; only use a URL that begins with "https" to connect your browser to the provider. Your information should also be protected and verified at all times using industry-standard protocols like IPSec (Internet Protocol Security), which are specifically designed to safeguard Internet traffic.

Service interruption:

Service outages are not unique to cloud settings, although they are more severe in this scenario, as shown in many cases [10-12], because to the interconnections between systems (e.g., a Seas utilizes virtualized infrastructures provided by an Iasi). This emphasizes the need of having strong disaster management strategies and service guidelines in place to ensure customer-side redundancy when required.

IV. Critical Evaluation

From the beginnings of cloud computing to its current state:

Forerunners of cloud computing emerged decades ago, first as time and compute sharing on mainframes, then as utility computing through private network providers. When the Internet was first established in the late 1990s, application service providers (ASPs) and grid computing gained traction. Both of them, however, had to deal with limitations, the most significant of which was a lack of network bandwidth to make them operate for large numbers of users. Because of the internet, fiber-optic cable, improved applications, and other advancements, cloud infrastructure now has the resources and pipelines it requires, and has branched into public, private, and hybrid cloud systems. It is, however, early in the history of clouds.

Take the Lead with SMBs:

While the majority of organizations, large and small, have adopted cloud infrastructure in some way, small and medium-sized companies (SMBs) lead the pack in terms of the proportion of resources they depend on from the cloud. According to a recent Spiceworks research, more than 60% of SMBs responding to the poll are now using cloud-based services, with IDC forecasting a nearly 20% increase in spending on these services over the next five years [13].

Dealing with more dynamic clouds:

Growing consumer demand, shorter deadlines, the growth of mobile devices, and the bring-your-own-device (BYOD) age have resulted in a dynamic mix of major businesses' data center networks and public, private, and hybrid cloud providers for many huge corporations. Furthermore, the growth of large data presents a significant challenge in terms of both storage and processing power. In addition to these reasons, the benefits of cloud infrastructure's flexible scalability and pay-as-you-go drive cloud expansion in big organizations to better address these challenges.

Security Still the Main Source of Distrust:

Despite these advances and the benefits of the cloud paradigm, many major business programs are still hesitant to move to cloud services due to concerns about frameworks and data security. For many large corporations, mission-critical applications have remained in-house and under the supervision of IT. According to management consulting and technology services firm Trains, cloud-based platforms will only enable 30 to 40% of business functioning in the near future, with the remaining 70 to 60% relying on technologies provided by in-house IT.

Inside the Firewall, More Gathering Clouds:

When IT continues to convert internal networks into more flexible and cost-effective private cloud providers, surveys show that internal and virtual clouds are frequently used.

There will be more cloud-based core market applications.

With the introduction of new technologies and platforms that enable the supply of complete physical servers while maintaining the ease and automation that cloud services provide, mission- critical applications will become increasingly cloud-based.

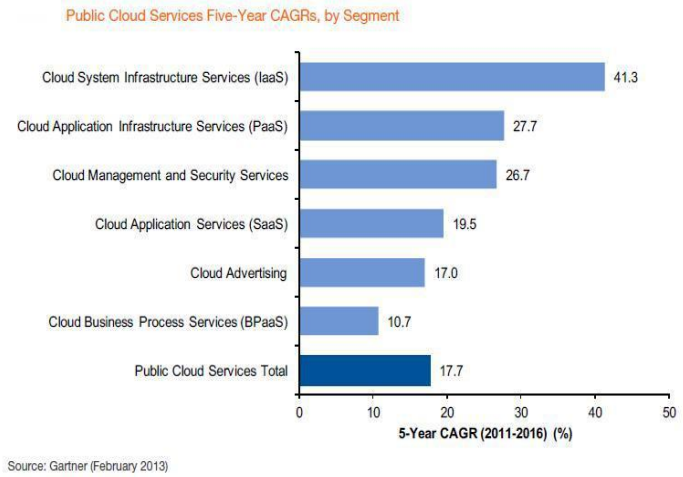

Figure no 2: Evaluation of cloud computing

V. Cloud success relies on automation and fast configurability

To promote prospective adoption, cloud services must offer the following: the capacity to offer hybrid platforms that seamlessly combine private and public cloud computing resources; the ability to provide virtual and physical infrastructure to support a wide range of applications, including mission-critical apps that need high performance; strong user self-service capabilities with a high degree of user self-service.

Cloud Computing Security Measures:

In view of Cloud Computing's significant security issues, this article outlined various appropriate response strategies.

Increase the ability to prevent attacks:

Cloud-based anti-attack hardware, anti-virus software, and firewalls are all possible. Several security companies have developed "cloud security," "cloud antivirus," and other applications.

Information security is a priority:

To increase the value of data in the cloud, we suggest shifting from shielding data from the outside (systems and applications that use the data) to shielding data from the inside. Information-centric [14] refers to a method of dealing with data and knowledge that maintains itself. This self-defense entails embedding intelligence in the data itself. Information must be self-described and defended, independent of its context. Data must be encrypted and packaged according to an use policy. When data is accessed, it should review its rules and try to re-create a secure environment via virtualization, exposing itself only if the environment is deemed trustworthy (using Trusted Computing). Information-centric security is a natural extension of the trend toward quicker, stronger, and more accessible data privacy.

Information Encryption:

Enabling data protection for all cloud data is a new way to ensure data access. The problem is that encryption limits data access. The data search and indexing are very difficult. If data is kept in clear-text, for example, you may efficiently search for a record by specifying a keyword. This is difficult to accomplish using conventional, randomised encryption techniques. State-of-the-art encryption may provide new methods to address these issues. Cryptographers have recently developed flexible encryption methods that make cipher text activity and calculation easier.

Cloud data proliferation may potentially enable better insider vulnerability monitoring (e.g., by recognizing user behaviors that are out of the ordinary) and better data loss prevention (DLP) since the cloud service provider has some capability to check for encrypted data (e.g., through detecting anomalous content).

In addition to preserving anonymity, applied cryptography may frequently offer resources to address additional security issues related to cloud storage. In order to prove irretrievability, the storage server must provide compact evidence that it properly retains all of the client's data.

High-Assurance Attestation for Remote Servers:

Customers must be satisfied with cloud services utilizing manual auditing techniques such as SAS-70 at this time.

The basis for a potential solution to this issue is Trusted Computing. Consider a controller placed on a trustworthy cloud server that can monitor or examine the cloud server's operations. The dependable monitor may give "proof of compliance" to the data owner, stating that such access restrictions have not been violated. In order to preserve monitor integrity, Trusted Computing typically allows safe bootstrapping of this monitor to run alongside (but securely detached from) the operating system and applications. The supervisor will establish access management policies and perform monitoring and auditing responsibilities. The monitor's code is signed in order to generate a "proof of compliance" and a "statement of compliance" from the monitor. When the data user has this proof of enforcement, it will verify that the appropriate display code is active and that the cloud service complies with access control rules.

Choosing an appropriate storage location:

Users have no idea where their data is handled since they depend on cloud storage, which poses additional security risks. Most intruders will be kept at bay by firewalls, monitoring, and intrusion avoidance, and data protection will keep the data secure, so we won't know where the data goes if our service or the cloud firm goes out of business. Dedicated hardware is the key to cloud infrastructure systems passing the most stringent safety requirements. As a result, they may choose reputable service providers in the same way that customers select cloud storage providers, and they should carefully read the privacy policies.

Establishing universal safety standards:

Several governments and organizations are now aware of the problem, and they are interested in investigating the development of a common standard to promote the use of cloud computing. Security requirements may include safety criteria for the creation of a protected mechanism for the security of privacy, in addition to technical standards.

Selecting dependable equipment suppliers:

Given their own long-term development and integrity, you may assess them with any necessary security measures in place by knowing which server and data center the data is being stored at. A business with sophisticated technical and operational capabilities would not disclose user information.

VI. THOUGHTS AND FUTURE PROJECTS

The problem of cloud protection management is something we're looking at. Our goal is to prevent the cloud paradigm from being adopted by cloud users' and cloud providers' security management systems. To solve this problem and provide cloud providers and customers with information on the current security status, we need to collect numerous protection criteria from various perspectives and layers of data and map security requirements to cloud infrastructure, security patterns, and compliance regulation processes.

Offering a safe platform and therefore allowing cloud technologies to be used and data and business activities to be moved to virtualized infrastructures requires protection. Many of the security issues discovered are commonplace in most computer environments: permission, network security, and regulatory requirements, for example, are not novelties. However, because of characteristics like multi-tenancy and resource sharing, the impact of such issues is magnified in cloud computing, since a single client's actions may affect all other users who ultimately use the same services and interfaces. Effective and reliable virtualization, on the other hand, presents a new challenge in this environment of increased delivery of dynamic networks and web-based applications, requiring more sophisticated methods.

It is important to create new frameworks that have the required protection standard by separating virtual machines and associated infrastructure while implementing best practices in terms of legal laws and enforcement with SLAs. Detection of virtual machines, adequate distinction of devoted resources combined with constant monitoring of mutual resources, and analysis of any attempt to influence cross-VM and data leakage are some of the criteria that may be used in such systems.

VII. CONCLUSION

The cloud is vulnerable to a variety of security vulnerabilities, ranging from network-level attacks to device-level threats. In order to keep the cloud secure, these security concerns must be managed. Furthermore, cloud-based data is often exposed to a variety of risks and difficulties, including security concerns, interoperability issues, anonymity, and data privacy. Both the cloud service provider and the user may ensure that the cloud is safe against any external threats, allowing the client and the cloud service provider to have a mutual understanding.

Furthermore, cloud service providers must ensure that all SLAs are met and that human errors on their end are minimized, allowing for seamless operations. This article discusses several security issues relating to the three main resources provided by a cloud storage system, as well as methods for avoiding them.

References

[1]. Song, D., Wagner, D., and per rig, A. Practical Techniques for Searches on Encrypted Data. In IEEE Symposium on Research in Security and Privacy. 2000.

[2]. L. Wang, G. Laszewski, M. Kunze and J. Tao, "Cloud computing: a perspective study", J New Generation Computing, 2010, pp 1-11.

[3]. Harjit Singh Lamba and Gurdev Singh, "Cloud Computing-Future Framework for emanagement of NGO's", IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.

[4]. R. Maggiani, Communication Consultant, Solari Communication, "Cloud Computing is Changing How we Communicate," 2009 IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, July 19- 22, 2009. ISBN: 978-1-4244-4357-4.

[5]. Ertaul, L. and Singhal, S. 2009. Security Challenges in Cloud Computing. California State University, East Bay.

[6]. http://computer.howstuffworks.com/internet/basics/internet-infrastructure.htm

[7]. An Information-Centric Approach to Information Security. http://virtualization.sys-con.com/node/171199.

[8]. http://www.idc.pt/resources/PPTs/2007/IT&Internet_Security/12.EMC.pdf

[9]. Boneh, B., Di Crescenzo, G., Ostrovsky, R., and Persiano, G. Public Key Encryption with Keyword Search. In EUROCRYPT. 2004.

[10]. Boneh, D and Waters, B. Conjunctive, Subset, and Range Queries on Encrypted Data. In The Fourth Theory of Cryptography Conference (TCC 2007), 2007

[11]. Shen, E., Shi, E., and Waters, B. Predicate Privacy in Encryption Systems. In TCC. 2009.

[12]. Shi, E. Bethencourt, J., Chan, H., Song, D., and Perrig, A. Multi-Dimensional Range Query over Encrypted Data. In IEEE Symposium on Security and Privacy. 2007.

[13]. TrendMicro (2010) Cloud Computing Security - Making Virtual Machines Cloud-Ready. Trend Micro White Paper

[14]. Genovese S (2009) Akamai Introduces Cloud-Based Firewall.http://cloudcomputing.sys-con.com/node/1219023